

Biometrische Identitäten und ihre Rolle in den Diskursen um Sicherheit und Grenzen

Dokumentation der gleichnamigen Tagung am
30. November und 1. Dezember 2012

Auszug

Biometrische Identitäten und ihre Rolle in den Diskursen um Sicherheit und Grenzen

Kommentiertes Protokoll der Tagung

Andrea Knaut

1. Auftakt – »ein kurzes schwaches Lob der jetzigen höhern Paßwissenschaft«¹

Nur der Pass liefert eine »wahre *Monographie* eines Einzelwesens, auf einem einzigen Folioblatt«. Durch ihn

»unterscheide z. B. ich mich auswärts von sämtlichen Spitzbuben in der Welt; denn ich zeige meinen gestempelten Papier-Paß vor, worin (außer meiner Handschrift) steht, daß ich 5 Fuß und 10 Zoll lang bin, 59 Jahre alt, in Wunsiedel geboren etc., daß meine Stirn breit und hoch ist und mein Mund klein. Oder läßt es sich nur träumen, daß es gerade einen Spitzbuben geben könnte, auf welchen alles von mir so passete, daß wir einander deckten, wie geometrischgleiche Figuren, oder ineinander eingriffen, wie Kerbhölzer? Unmöglich! – Sogar meine nächsten Nachahmer und Diebe würde mein Paß, so sehr ich auch Swift und Sterne nachgeahmt und bestohlen, auf der Stelle unterscheiden von mir.«²

1 Wolfgang Coy beginnt die Tagung mit dem hier zitierten Auszug aus Paul, Jean, 1996: Der Komet. Nikolaus Marggraf. Eine komische Geschichte. In: Sämtliche Werke, Abt. I, Bd. 6, Zweitausendeins, S. 565-1036 (Erstausgabe: Verlag Georg Reimer, 1820-22). Im Internet abrufbar unter: <http://gutenberg.spiegel.de/buch/3203/1>.

2 Ebd.

Wie wäre Jean Pauls ironische Bewunderung des Ausweisdokuments noch gesteigert worden, hätte es die heute übliche Speicherung der Körpercharakteristika in Form sogenannter biometrischer Merkmale in Pässen und die automatische Personenerkennung schon gegeben. Vielleicht wäre ihm dies als brauchbare Realisierung seines Traums erschienen, dass

»die Polizei allgemeine Pässe – etwa nach der ersten Beichte – auf den Rücken aller Volljährigen, als zweite Taufscheine, mit Geburtort, Eltern u. s. w. so einbrennen könnte, daß mans mehr sähe als spürte.«³

Ein solcher Einfalle zeige nämlich, dass sich

»ein eingetätztes Paß- oder Flebbswesen ebensogut mit feinstem Ehrgefühl (trotz allem Anscheine von Brandmarken) vertrage als mit Ersparung von Schreibgebühren, Zeitaufwand und mehr dergleichen.«⁴

Die Biometrie wird oft als Instrument gesehen, den menschlichen Körper selbst zum Ausweis zu machen – eine biopolitisch subtile Brandmarkung also?

Biometrie sei ein Thema, so Coy in seinem Einführungsvortrag, das die Arbeitsgruppe *Informatik in Bildung und Gesellschaft* fast schon immer beschäftigt habe. Nur hätten sich die damit verbundenen Projekte dann doch meist in eine andere Richtung entwickelt, weil es ein sehr schwieriges, ein sehr schlecht greifbares Thema sei. Er nennt es eng verbunden mit dem »Problem der Identität«. Und mit diesem aber ist

3 Ebd.

4 Ebd.

»ein philosophisches Faß ohne Boden aufgemacht: Der Begriff der Identität ist so kompliziert, dass man ihn sicher mit technischen Mitteln leicht lösen kann. Deswegen gibt es die Biometrie, wo zumindest in irgendeiner seltsamen Variante angedeutet wird, man könne Menschen so vermessen, dass sie identifizierbar sind.«

II. »Europäische Biometrie im 19. Jahrhundert: Semiotische Identitäten in Kriminologie und Kriminalistik«⁵

Die Einführung biometrischer Methoden, beginnt Miloš Vec mit seinem Vortrag, hätte um 1900 in der »Wissenschaft [...] der Tataufklärung«, der Kriminalistik, »einem semiotischen Geschäft«, einen Bruch mit den bisherigen Praktiken in diesem Bereich dargestellt. Kriminalistinnen sammeln, sichten und interpretieren Zeichen oder Spuren. »Der Kernbereich des Identifizierungsgeschäftes betrifft [...] klassischerweise die Aufklärung von Straftaten.« Die Identifizierung von Personen wird allerdings im 19. Jahrhundert zu einem sich verschärfenden Problem, verursacht durch »die Verstädterung, die gestiegene Mobilität der Bevölkerung sowie das Erscheinen des modernen Interventionsstaates«. In diesem lautet das »Versprechen auf Sicherheit und Wohlstand, zwei Begriffe die Schlüsselmotive aller Staatstheorie und Fluchtpunkt der Zweckbestimmungen sind.«

5 Vortrag von Miloš Vec vom 30.11.12.

Auch die Identitätsfeststellung dient der Sicherheit und dem Wohlstand. Sie verbindet »zivilgesellschaftliche und strafrechtliche, staatliche Interessen«.

Die Liste der Standardinstrumentarien zur Personen-erkennung erweitert sich rasant in der zweiten Hälfte des 19. Jahrhunderts: Traditionell gibt es bereits die Steckbriefe, die textuelle Erläuterungen oder Zeichnungen menschlichen Aussehens enthalten und zunächst oft subjektiv und wenig normiert sind. Insbesondere im nachrevolutionären Frankreich finden Pässe mit genauen Angaben zu Namen, Geschlecht, Alter und Angaben zum Äußeren zunächst Verbreitung. Die Polizeien Europas und der Vereinigten Staaten führen Verbrecherakten mit Personenbeschreibungen ein. Daguerreotypie und Fotografie erweitern diese um Porträtfotos. Aber vor allem treiben die Anthropometrie oder schließlich die Daktyloskopie den Bedeutungszuwachs der kriminaltechnischen Indizienbeweise an. Das Vorverfahren, führt Vec weiter aus, habe bald als reine Stoffsammlung gegolten und die Verdächtige sei ein Beweismittel im eigenen Verfahren geworden. Die Technisierung der Ermittlungsverfahren habe dieses Problem verschärft, und die Kontrolle der Beweisführung sei nach und nach auf die Polizeien übergegangen. Allerdings hätten lange Zeit »Standards und Verfahren der Ermächtigung und der Kontrolle« gefehlt. Ihre »Vergesetzlichung« sei bis zur Jahrhundertwende vom 19. zum 20. Jahrhundert ausgeblieben. Eine Legalisierung der ohnehin schon verwendeten Verfah-

ren des kriminalistischen Erkennungsdienstes habe in Deutschland beispielsweise 1933 mit Paragraph 81b der Strafprozessordnung nachholend stattgefunden.

Insgesamt verliert also vor allem das Beweismittel der Zeugenaussage mit den Entwicklungen des 19. Jahrhunderts im Verhältnis zum »Kronjuwel Sachbeweis« erheblich an Bedeutung. Dieser »Aufstieg des Sachbeweises« und der Bedeutungszuwachs der Wissenschaftszweige Kriminalistik und Kriminologie sei von einem »Rechtfertigungsnarrativ imaginierter Gefahrenpotenziale« begleitet. Es findet eine zunehmende »Verwissenschaftlichung des polizeilichen Erfahrungswissens« mit einer »Obsession [für] terminologische Differenzierung« statt. Ob nun in der Beschreibung besonderer körperlicher Merkmale, der Polizeifotografie, der anthropometrischen Bertillonage oder der Daktyloskopie, es sich lasse im 19. Jahrhundert immer wieder die »Affinität für technokratische Lösungen« als eine Entwicklungslinie erkennen. In dieser Epoche entstehe die zentrale Bedeutung »semiotischer Identität« innerhalb der Kriminalistik, die bis heute auch die Basis digitalisierter Identitätsbeweise innerhalb biometrischer Systeme ist.

»Identität bezeichnet neben der Übereinstimmung von Sachen insbesondere auch die Vorstellung des äußerlich oder innerlich unveränderlichen Wesenskerns einer Person. Eine Identifizierung vorzunehmen bedeutet die Zuweisung einer Identität zu einem Körper.«

Das bedeutet, wie Vec es später noch etwas anders ausdrückt, dass »erst im Moment der Identifizierung [...] eine Konstruktion von Identität stattfindet.«

In der Biometrie wird davon ausgegangen, dass bestimmte unabänderliche, einmalige und universelle Körper- oder Verhaltensmerkmale konstitutiv für eine menschliche Identität sind. Heute werden im Massengebrauch praktisch vor allem Fingerbilder, Gesicht, Iris, Handgeometrie, Stimme oder Hand- bzw. Unterschrift als derartige biometrische Charakteristika genutzt. »Das biometrische Versprechen lautete und lautet bis heute: Die Natur wiederholt sich nicht.« Ironischerweise wiederholt sich auch das Ergebnis einer Messung nicht: Jeder Messvorgang selbst verfälscht das Abbild (Muster) des vermeintlich originalen Charakteristikums stets in einer Weise, dass es nie als dasselbe wiederkehren kann. Die Kunst besteht für die Ingenieurinnen und Programmiererinnen darin, den Messfehler zu minimieren. Könnte es sich also wie schon bei der verheißungsvollen vermeintlich realistischen Fotografie in der Wende zum 20. Jahrhundert erweisen, dass die »Repräsentationen des Identischen« nicht identisch sind oder, schwächer ausgedrückt, dass die genügende »Selbstähnlichkeit« fehlt?

Zumindest bis heute und vermutlich auch in naher Zukunft behält die »Mess-Guerilla« die diskursive Oberhand, vereint in »Fortschrittsoptimismus und männliche[r] Technophilie«.

Die kriminalistischen Methoden sind auch stets als Teil systematischer Erläuterungen in der Ursachen- und Präventionsforschung für kriminelles Verhalten, der Kriminologie, genutzt worden. Vec aber behauptet, der Preis etwa der Daktyloskopie sei der Bedeutungsverlust der mit dem biometrischen Signalement verknüpften »kri-

minogenen Dispositionen [...], die Stigmata der Devianz von Lombroso, den Phrenologen und Kriminologen« oder Rassenkundlerinnen. An anderer Stelle weist Vec zwar darauf hin: »Die Anthropometrie hat etwa eine unrühmliche, koloniale Geschichte, in der sie mit der Rassenkunde verbandelt war.« Doch er sieht diese Ausprägungen klar der Vergangenheit zugehörig. Die Hermeneutik in der Kriminologie sei eliminiert worden:

»Die Zeichen sollten weder auslegungsbedürftig noch kriminologisch auslegungsfähig sein. [...] Das biometrische Geschäft hatte den Sinn für die sichtbaren körperlichen Zeichen sozialer, rechtlich relevanter Devianz aufgegeben. Diese leben heute eher in Parawissenschaften, Massenmedien, Physiognomik, Graphologie in hochgradig diskriminierenden Ausformungen fort.«

Doch die Verbannung der kriminogenen Disposition, von der Vec hier spricht, ist nur eine scheinbare. Die Unterstellung der Disposition ist im Gegenteil universell und Voraussetzung für den Gebrauch biometrischer Charakteristiken. Es ändern sich lediglich die Deutungskontexte: Biometrische Erfassung kann beispielsweise auf bestimmte soziale Gruppen beschränkt werden oder Verhalten, Hautfarben, körperliche Dispositionen beabsichtigt oder unbeabsichtigt differenzieren. Dies geschieht weniger nachvollziehbar, und nicht mehr offensichtlich von konkreten Akteuren verantwortet, die weiterhin aufgrund rassistischer, klassistischer oder sexistischer Herrschaftspraktiken diskriminieren. Dessen unbenommen verbinden sich nicht von vornherein bössartige, menschenfeindliche Absichten mit der Forschung an der

Biometrie. Viele Kriminalistinnen oder Informatikerinnen erträumten und erträumen sich mittels Biometrie wissenschaftlich fundiertere Urteile in somit aus ihrer Sicht gerechteren Gerichtsverfahren oder versprechen sich von der sogenannten ‚Anonymen Biometrie‘ einen verbesserten Persönlichkeitsschutz.

Für Staaten und Obrigkeiten sei das »Identifizierungsgeschäft« nicht nur hinsichtlich der Aufklärung von Straftaten und Ordnungswidrigkeiten oder des Erkennens unbekannter Toter interessant, sondern auch für die Kontrolle der Mobilität bei Ein- und Ausreise und der Teilhabe Einzelner an sozialen Sicherungssystemen.

Auch Privatunternehmen markieren Kundinnen heute mit Ausweisen, Payback-Karten, Armbändchen oder Funk-Chips. Sie erstellen eigene Steckbriefe, in ihrem Jargon: Profile, installieren Kameras und sammeln persönliches Material.

In allen Lebensbereichen lege der »Fokus auf Wiedererkennung« von zur Teilhabe Berechtigten. Dies sei sowohl kulturell durch gesellschaftliche Grundannahmen über »Tätertypen, Bedrohungsszenarien, Gewohnheitsverbrecher« und die damit verbundene kalkulierbare Wiederkehr von Straftaten als auch »technisch induziert«. Im modernen »Präventions- und Prädiktionsstaat« würden zudem »schichtspezifische Verdachtsmomente« institutionalisiert. Das Bürgertum sei zunächst dem Verdacht kriminogener Neigungen entzogen gewesen. Diese »alte Dichotomie« – brave Bürgerinnen und böse Verbrecherinnen – habe bis in die neuere Zeit die »Akzeptanz einer ‚Volksdaktyloskopie‘« in manchen Staaten gesenkt. An-

ders verhält es sich dagegen mit der Unique Identification Authority of India (UIDAI) oder der National Database and Registration Authority (NADRA) in Pakistan. Diese Behörden verwalten die größten Biometrie-Datenbanken der Welt, in denen sie sämtliche Staatsbürgerinnen erfassen.

Schließlich konstatiert Vec doch:

»[Weltweit] keimt erneut der Wunsch auf, naturwissenschaftlich-technisch dennoch etwas über die bösen Neigungen von Individuen zu erfahren. [...] Die Vergleichen findet dann [...] mit dem Normalfall des unverdächtig Guten statt, von dem aus die physiologische Abweichung zum Verdacht böser Absichten führt. [...] Kriminologie und Kriminalistik verhandeln ihr Verhältnis angesichts der aktuellen biometrischen Revolution neu.«

Und so ist es kaum überflüssig, am Ende eine Aussage des Vortrags noch einmal besonders zu hervorzuheben:

»Identifizierungspflichten sind in einer freiheitlichen Gesellschaft rechtfertigungsbedürftig. Anonymität ist ein mit der Meinungsfreiheit verknüpft Grundrecht.«

III. »How to liquefy a moving body: Eurodac und die Digitalisierung der Europäischen Grenze«⁶

Die Grenzbiometrie ist Teil der massenhaften Vermessung der Weltbevölkerung zum Zwecke ihrer besseren Kontrollierbarkeit in hoheitlichen Kontexten. Die biometrische

6 Vgl. Manuskript des Vortrags vom 30. 11. 12 von Brigitta Kuster und Vassilis Tsianos in diesem Band, Seite 19 (Zitate in diesem Kapitel sind aus selbigem).

trischen Maßnahmen sind dabei in komplexe Regelwerke eingebettet. Eines ist die Dublin-II-Verordnung der Europäischen Union (EU),⁷ die das »Regulativ der Mobilität von Nicht-EU-Staatsbürger_innen ohne Visum innerhalb der EU« darstelle, so Brigitta Kuster und Vassilis Tsianos. Das technische Hilfsmittel dazu, das europäische Fingerabdruckidentifizierungssystem Eurodac, soll absichern, »dass der Mitgliedstaat, der die Einreise eines_r Asylantragssteller_in „verursacht“ hat (etwa durch Vergabe eines Visums oder aufgrund mangelnder Sicherung der Grenze), das Asylverfahren durchführen muss.«⁸ Kuster und Tsianos untersuchen in ihrer Forschung diese »digitale Grenze« als soziotechnologisches Objekt. Wenn »Kontrolltechnologien zur Grenzsicherung [...nur] in ihren politischen Wirkungen erfasst und kritisiert« werden, blieben die Technologien wie Eurodac zunächst selbst opak und »potenziell funktionstüchtig«. Eine solche Analyse folge »einer Art Blackbox-Epistemologie«. Mit einer ethnografischen »De-Blackboxing-Operation«, die auf die menschliche Konstruktion und Nutzung der

7 Diese Verordnung erfreut sich inzwischen der dritten Überarbeitung. Im Jahr 2003 ersetzte die Dublin-II-Verordnung (EG) Nr. 343/2003 das Dubliner Einkommen von 1990. Seit Mitte 2013 ist die Dublin-III-Verordnung (EG) Nr. 604/2013 in Kraft, weiterhin »zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist«.

8 Zu Eurodac siehe Absatz XII.

Informationstechnologie abhebe, lasse sich aber hier auch soziologisch noch weiter gehen.⁹

Die in kategorisierten Mustervergleichen des Identifizierungssystems Eurodac hervorgebrachten Zahlen etablierten, so Kuster und Tsianos, eine »verkörperte Identität der Migration«. Sie würden zu »Bedeutungs- und Legitimationsträgern« für paramilitärische Grenzkontrollaktionen wie die der Rapid Border Intervention Teams (RABIT) an der griechisch-türkischen Evros-Grenze. Dass diese Zahlen alles andere als objektiven Charakter haben, zeigt sich im Interview der beiden Forschenden mit einem Beamten des Bundeskriminalamts (BKA). Der Beamte wundert sich im Gespräch über die Eingabep Praxis der Griechen bei der Nutzung von Eurodac und macht einen strategischen Vorschlag, mit welcher Art der Dateneingabe sie »viele Asylbewerber loswerden« könnten.

Doch »Bewegung kommt vor ihrer Kontrolle« – Tsianos und Kuster versuchen zu privilegieren, was eine Grenzkontrolltechnik aus dem Blick verliere: das »Wissen der Migration«, das Wissen der Betroffenen und ihre Erzählungen. In ihren ethnografischen Studien seien sie etwa einem Einwanderer namens Rastaman in der heute von der Polizei zerstörten informellen Siedlung Igoumenitsa begegnet, der davon gesprochen habe, wie er »befragt, fotografiert und ‚gefingert‘« wurde. Die mit dem letzten Begriff gemeinte Abnahme der Fingerabdrücke wird so-

9 Ein technisches De-Blackboxing ist auch Aufgabe der ethisch umsichtigen Informatikerin. Siehe dazu den Text von Oepen, Seite 37, bzw. Absatz V für dessen kurze Zusammenfassung sowie die Zusammenfassung des Beitrags von Hansen in Absatz IV.

wohl auf Papier als auch auf einer Glasplatte durchgeführt. Das Glas sei ein Gegenstand, der wiederholt als gefährlich in den migrantischen Geschichten auftauche.

Die Exklusion mittels der digitalen Grenze, die die Migrantinnen nun am Körper trügen, sei, nach Dennis Broeders, zum einen die »von der Registrierung bzw. Dokumentation« als Rechtssubjekte und zum anderen die »durch Registrierung bzw. Dokumentation« als Rechtlose (Hervorhebung der Autorin). Das Wechselspiel zwischen beiden Formen der Ausgrenzung »bildet Konjunkturen der 'digital deportability' heraus«, die »die Risiken der Mobilität – Geld, Ausdauer, Länge des Unterwegs-Seins und manchmal das Leben selbst« – bedeute. Die »verkörperte Identität der Migration« ist die Summe der »Eurodac-Datenkörper«:

»Sie machen die mobilen und flüchtigen Körper der Migrant_innen, die sie inskribieren, nicht nur maschinenlesbar und verifizierbar, sondern auch fluid und hypermobil.[... Migrant_innen tragen] die Grenze zugleich mit sich, wie sie dagegen verstoßen.«

Eine interessante Nebenbemerkung machen Tsianos/Kuster zu einem technischen Aspekt der biometrischen Erkennung: In dem System werden Treffer nach einer sogenannten 1:N-Suche gefunden, bei der ein Muster gegen viele in der Datenbank abgelegte verglichen wird. In der Biometrie wird ein solcher Suchprozess als *Identifizierung* definiert, während eine 1:1-Suche nach hinreichend deckungsähnlichen Mustern als *Verifikation/Authentifikation* bezeichnet wird. Die Autorinnen deuten dies als eine

»im westlichen (Alltags-)Denken übliche Unterscheidung [...] zwischen Wahrheit und Identität. Während die Wahrheit zu erlangen dem Versuch entspricht, die Vermittlung zu liquidieren und auf diese Weise Deckungsgleichheit zu erreichen, ist Identität immer schon konfrontiert mit den Schwierigkeiten des Prozesses, Vielheit abzuziehen. Authentizität wiederum versucht, die Subtraktion der Vielheit der Identität im Singulären anzutreffen.«

Diese schwer zu verstehenden Sätze, die allzu beiläufig in eine Fußnote gesteckt worden sind, thematisieren die kulturelle Verankerung der Verbindung zwischen biometrischen Mustervergleichen und *einer* wahren Identität, in der Vielheit nicht sein darf. Der Text von Herbert Hrachovec in diesem Bändchen vertieft derartige dem Identitätsbegriff zugrundeliegende erkenntnistheoretische Annahmen.¹⁰

IV. »Biometrie in Zeiten von eIDs, Social Networks und Cloud Computing – die Datenschutzsicht«¹¹

Eine informatische Herangehensweise, die der von Tsianos und Kuster beschriebenen Methode des *De-Blackboxing* als Technikdokumentation ähnelt, ist die des Datenschutzes. Diese Perspektive nimmt Marit Hansen ein. Sie erklärt, um das Recht auf informationelle Selbstbestimmung als elementares Schutzrecht des Einzelnen überhaupt aufrechtzuerhalten, »muss jeder natürlich

10 Vgl. Hrachovec, Seite 3, kurz zusammengefasst in Absatz IX.

11 Vortrag von Marit Hansen vom 30.11.12.

auch wissen, was jemand über ihn weiß«. Das erfordere »Transparenz« im Sinne von Verständlichkeit der Technikfunktionalitäten und Auskunftangebote darüber, sowohl für Laien als auch für Experten. Außerdem müsse »Intervenierbarkeit« sowie die Infragestellung einer datenverarbeitenden Blackbox möglich sein. Ein Individuum dürfe dem System nicht einfach ausgeliefert sein.

Aus Datenschutzsicht sei Biometrie zumeist das »Gegenteil einer Hochsicherheitstechnik«, wozu sie oft erklärt würde. Es gebe viele intransparente Manipulationsmöglichkeiten, beginnend bei der Ersterfassung, dem Enrolment, der Daten, über deren Übertragung bis hin zu deren Abgleich. Vor allem das Prinzip der Intervenierbarkeit sei im Falle eines Systemfehlers kaum gegeben. Auch die lebenslange Bindung der biometrischen Daten an die Person sei hochproblematisch.

Hansen weiß aus ihren Erfahrungen als Mitarbeiterin des Unabhängigen Landeszentrums für Datenschutz in Schleswig-Holstein eine Anekdote über die heimliche und nicht bemerkbare Neukonfiguration eines biometrischen Systems eines Geldautomaten zu berichten. Das System wies häufig fälschlicherweise eigentlich zur Finanztransaktion berechnigte Kundinnen als Identitätsbetrügerinnen ab. Die Bank entschied sich daraufhin, das System kurzfristig derart zu manipulieren, dass es für 24 Stunden einfach jede Kundin als Zugangsberechtigte akzeptierte. Man habe die Folgen, die aus den Beschwerden über die unberechtigten Rückweisungen durch das nicht funktionierende Identifizierungssystem entstan-

den wären, für geschäftsschädigender gehalten als einige wenige mögliche Falschakzeptanzen von unberechtigten Kundinnen. Dieses Beispiel zeigt mehrerlei: Die Betroffene weiß nie, wie der Schwellwert für hinreichende Ähnlichkeit zweier Muster, die ihr den Zugang zu einem durch Biometrie kontrollierten System erlaubt, zu einem bestimmten Zeitpunkt eingestellt ist und bemerkt eine administrative Manipulation dessen nicht. Die Betreiberinnen eines solchen Systems erhalten im Zweifel den Glauben an dessen Funktionieren auch dann aufrecht, wenn sie es außer Kraft setzen. Das können sie, weil es sich um eine Blackbox handelt. Ferner gehen sie, zumindest in diesem kleinen Zeitfenster, davon aus, dass die meisten Kundinnen ohnehin in ehrlicher Absicht nur ihr eigenes Geld abheben möchten.

Ein weiterer besorgniserregender Aspekt sei aus datenschutzrechtlicher Perspektive, dass wesentlich mehr darüber geforscht werde, welche Zusatzinformationen biometrische Daten über bestimmte körperliche oder verhaltensbezogene Dispositionen offenbaren, als dazu, wie sich derartige Zusatzinformationen verbergen und verhindern lassen. Eine potentielle Krankheitserkennung oder das Erkennen einer ethnischen Herkunft mittels Wahrscheinlichkeitsanalysen werde in den gängigen Implementierungen nie prinzipiell ausgeschlossen.

»Bis 5 %, so die Daumenregel«, betrage außerdem der Anteil der Personen, bei denen die gängigen biometrischen Verfahren nicht funktionieren.

Hinzukommen viele weitere Probleme. Beim Reisepass seien retuschierte Fotos einreichbar. Es gebe keine internationalen Standards für die Art der Auswertung der biometrischen Daten an unterschiedlichen Grenzkontrollpunkten. Es würden Rohdaten gespeichert.

All dies sind Belege dafür, wie überstürzt biometrische Systeme im Reiseverkehr eingeführt und auf diese Weise einfach Fakten geschaffen wurden.

Einer der Versuche, Regeln für eine datenschutz sensible Implementierung von biometrischen Systemen zu schaffen, sei die »Stellungnahme 3/2012 zu Entwicklungen im Bereich biometrischer Technologien« der Artikel-29-Datenschutzgruppe der EU vom April 2012.

V. »Transparenz und Datensparsamkeit von elektronischen Ausweisdokumenten in Deutschland«¹²

Exemplarisch für eine zentrale Komponente eines biometrischen Systems sind Ausweisdokumente als Datenträger biometrischer Merkmale. Der Informatiker Dominik Oepen beschäftigt sich in seinem Vortrag mit der Frage der technischen Realisierung des Schutzes der auf den Radio-Frequency-Identification-(RFID-)Chips der Pässe gespeicherten Daten. Diese könnten kontaktlos und damit auch durchaus unbemerkt ausgelesen werden, theoretisch über »Reichweiten von 40 bis 50 Zentimetern«.

12 Vgl. Transkript des Vortrags von Dominik Oepen am 30.11.12 in diesem Band, Seite 37.

Eine bereits »bestehende Kommunikation mit einem Dokument und einem Lesegerät [...lässt sich] auch über eine Entfernung von mehreren Metern« belauschen.

»Die Einführung elektronischer Ausweisdokumente in Deutschland erfolgte schrittweise.« Zuvor sei die sogenannte »eCard-Strategie des Bundes« beschlossen worden, um die Verbreitung von Chipkarten »in allen Bereichen von eBusiness und eGovernment« und »vor allem elektronische Authentisierungsdienste und elektronische Signaturdienste« zu fördern. Die eID-Funktion des Ausweises, die etwa Internetgeschäfte sicherer machen soll, sucht man akzeptanzfördernd datensparsam umzusetzen. Dazu gehört beispielsweise, dass für den Zugriff auf Ausweisdaten Zertifikate nötig seien. Diese können Diensteanbieter bei der Vergabestelle für Berechtigungszertifikate erhalten. Sie müssten dazu transparent glaubhaft machen, warum sie welche Daten für ihre Zwecke beim Ausweisinhaber auslesen. Man kann nur »spekulieren, wie gut diese Prüfung tatsächlich erfolgt«. So gebe es, sagt Oepen, »einige Dienste in der freien Wildbahn, wo man sich fragt: Wie sind die denn damit durchgekommen?«

Die eID-Funktion bürokratisiert die in Tauschgeschäften nötigen Vertrauensentscheidungen auf eine unnötige Weise. Zudem ist das Ganze halbherzig umgesetzt: Hoheitliche Systeme wie Grenzterminals sind ausgenommen von der Datensparsamkeitsregelung. Mit ihnen lasse sich auf alle auf dem Ausweischip gespeicherten Daten zugreifen.

Beim elektronischen Aufenthaltstitel wird die neue Qualität der Bürokratisierung durch digitale Systeme ebenfalls deutlich: Die seitens des Staates erforderlichen Aufenthaltstitel seien früher »einfach Aufkleber in den nationalen Reisepässen« gewesen. Nun seien es Chipkarten, die dem Inhaber dieselben Funktionen wie der Personalausweis bieten (oder vielleicht doch: aufzwingen?) und die Abgabe zweier Fingerabdrücke bedingen. Eine vollends kriminalistische Praxis in Kombination mit erhöhter Unsichtbarkeit der Speicherung und des Abrufs von Daten, die ein Ausweisdokument erst zu einem sinnvollen machen, institutionalisieren wohl eher das grundsätzliche Misstrauen einer staatlichen Institution gegenüber einzelnen Individuen.

Wie in der Informatik oft üblich beschreibt Oepen sämtliche Prozesse der nun durch Maschinen gefilterten Zugangskontrollsituation an Grenzen oder bei Geschäften mit personifizierenden Metaphern – es gibt sprachlich keinen Unterschied zwischen Mensch und Maschine:

»Mit der Chip-Authentication wird die Authentizität des Reisepasses nachgewiesen. Der Reisepass weist also nach, dass es sich um einen echten Pass handelt [...] In die andere Richtung weist das Terminal nach, dass es tatsächlich berechtigt ist, auf den Reisepass zuzugreifen. [...] Im weiter entwickelten PACE-Protokoll] muss zunächst der Dienstanbieter, bzw. das Inspektionssystem, nachweisen, dass es zum Zugriff auf den Ausweis berechtigt ist, bevor der Ausweis seine Authentizität nachweist.«

Der Anthropomorphismus inspiriert zu verschiedenen Feststellungen zur Durchdringung der IT-Systeme, die ja tatsächlich stets menschliche Interaktionen abbilden und wieder auf diese rückwirken:

Maschinelle Prozesse mit Referenz auf menschliche Aushandlungen zu erklären, macht sie verständlicher – zumindest oberflächlich. Sie appellieren an die alltägliche Erfahrung. Das Ritual, dem Grenzbeamten und Kontrollierte folgen, ist selbstverständlich bei genauerem Hinsehen ähnlich undurchsichtig wie das maschinelle. Die Handlungsparameter der Beteiligten sind gleichermaßen gekapselt in einer Blackbox. Die Kontrollsituation wird durch das Digitale nun um eine andere Blackbox der elektronischen Übertragungs- und Verschlüsselungsprotokolle erweitert. Sie sind nur oberflächlich einfach zu erklären und hochgradig störrisch.

Sie zu manipulieren ist Teil eines technischen Spiels, das sehr ernste Konsequenzen und Motive haben kann. Im Technikjargon gehört die Manipulation menschlicher Interaktion, das *social engineering*, zu einer breiten Palette der sogenannten Angriffsszenarien in IT-Systemen. Dass die Informatik-Systeme komplexe Situationen für Menschen kontrollierbarer machen, ist absurd. Doch ökonomisch ist das Spiel sehr lukrativ. Die Manipulation provoziert die Verbesserung des Manipulierten: Im Spiel mit sich selbst geht am Ende schnell der Blick für Ursache, Wirkung und Sinn einer derart elektronisch stabilisierten Identitätspolitik verloren.

VI. »BeID-Labor«¹³

In technischen Umsetzungen von sogenannten Identitätsnachweisen sind Reflexionen zu ihren historischen, kulturellen oder erkenntnistheoretischen Voraussetzungen nachrangig. Beispielsweise steht die der Biometrie zugrundeliegende Vereinfachung, dass ein Individuum mit Hilfe des Abgleichs von Mustern ein und desselben, bestimmten Anforderungen genügenden Körpermerkmals in allerlei Kontexten und über lange Zeit hinweg wiedererkennbar wäre, kaum zur Debatte. Schließlich sind die sich für das vermeintlich geschlossene technische Biometrie-System stellenden Probleme der Signalverarbeitung, -übertragung, der Effizienz des gesamten Systems und der Mustervergleichsalgorithmen, der Sicherstellung der Datenintegrität und des Schutzes vor Manipulation verzwickelt genug.

Genauso aber, wie es unmöglich ist, die Richtigkeit einer automatisierten Personenidentifikation automatisiert zu überprüfen, ist es sinnlos anzunehmen, dass die Biometrie und das Passwesen durch eine immer stärkere Verbesserung der Vergleichsalgorithmen, der Fälschungssicherheit von Ausweisen oder diverser Manipulationserkennungstechniken den gefürchteten Identitätsbetrug vollständig verhindern würden. Die Angst, es in großen Bürokratien, anonymen Städten oder Internetgeschäften mit den Falschen zu tun zu haben, denen zu vertrauen, die man nicht persönlich kennt, ist dennoch der Motor einer Identitätsindustrie und Sicherheitsforschung, die sichere Drittmittel garantieren. Wer

¹³ Vortrag von Wolf Müller vom 30.11.12.

die Falsche, Kriminelle oder die Angreiferin sein mag, ist historisch, sozial wie räumlich kontextabhängig. Aus Sicht der IT-Sicherheit ist die Angreiferin eine Metapher. Sie bedeutet eine imaginierte Person, die die Integrität und definierte Funktionstüchtigkeit einer datenverarbeitenden Maschine absichtlich stört.

Das *BeID-Labor*, das Wolf Müller vorstellt, steht exemplarisch für die Kooperationen zwischen Forschung, Staat und Industrie. Mit relevanten Ergebnissen der Forschung, »Studien-, Bachelor-, Master-, Diplomarbeiten, Patenten, Papers und Open-Source-Produkten« versorge die Hochschule – in diesem Fall die Humboldt-Universität – via »Industriekontakten« den deutschen Standort mit Technologie. Im Schwung der Innovationsorientierung ist die Verwendung eines bedeutungsgeladenen Begriffs wie *electronic IDentity* nicht mehr als ein Buzzword, das den Drittmittelgebern hingeworfen wird. Die Bereitstellung einer freien Programmierschnittstelle für den elektronischen Personalausweis – eines der zentralen Produkte des *BeID-Labors* – ist einerseits ein Schritt hinsichtlich dessen technischer Transparenz, andererseits eine Fortschreibung und Vertiefung der staatlichen Kontrolle des Individuums und der diskursiv vorherrschenden Sicherheits- und Präventionslogik.

VII. »Write Me Down, Make Me Real«¹⁴

Eine Person zu sein bedeutet einen Namen zu haben und von anderen gekannt zu werden. Es findet eine Zuordnung statt. Anonyme Personen sind ein Problem, sie lassen sich nicht zuordnen. In seinem Vortrag unternimmt Christoph Engemann einen geschichtlichen Exkurs zur Bedeutung der Namensgebung und ihrer Sammlung in großen Registern als identitätsstiftende Instrumente.

Die im Mittelalter beginnende Geburtenregistratur der Kirchen habe im Streit der Konfessionen eine »neuartige Verschränkungsstelle von Biomacht und Medien« gebildet: Pastoren seien im 16. Jahrhundert ab dem Konzil von Trient zu Sekretären geworden. »Die Taufe ist ein initialer Schreibakt in der Seele und zugleich auf dem Papier der Kirchenbücher.« Die Zugehörigkeit zur Christenheit werde so manifestiert.

»Gott [...] ist [vor diesem Hintergrund] ein Aufschreibesystem mit unendlicher Speicherkapazität, das die Gesamtheit des Tuns (und Lassens) der Menschen dokumentiert und am Tag des Jüngsten Gerichts abfragt.«

Die katholische Kirche lässt sich als »erste[...] und älteste[...] verfasste biopolitische Bürokratie der westlichen Welt« sehen, in der Geburt und Schreiben in einem »untrennbare[n] Verhältnis« stehen. Allerdings war die Handhabung der Geburtenregistratur bis zu deren Säkularisierung im 18. Jahrhundert wenig strikt. »In protestantischen Regionen fand sie ebenso wenig statt wie in jüdischen Glaubensgemeinschaften.«

14 Vortrag von Christoph Engemann vom 30.11.12.

Neben der Kirche habe auch die spanische Krone im 16. Jahrhundert die Präsenz des Königs in den südamerikanischen Kolonien abgesichert, indem sie von den dortigen Staats- und Kirchenvertretern ein permanentes Beschreiben »alle[r] Dinge und Ereignisse auf der anderen Seite des Atlantik [...] – ‚entera noticia de las cosas‘« – verlangte. Außerdem würden ab Mitte des 16. Jahrhunderts für jeden nach Nueva Espana eingeschifften Passagier Papiere zur Pflicht. Dies sei für nicht-adlige Menschen ein revolutionärer Schritt gewesen:

»Plötzlich galten normale Menschen des Schriftlichen würdig, erhielten Urkunden und Dokumente, ein Privileg, das sonst nur Adligen und vielleicht noch anderen wie Richtern zustand. [...] Verarbeitet wurden die anfallenden Dokumente in einer zentralen Einrichtung, der 1501 gegründeten Casa de la Contratación in Sevilla.«

Sowohl in der Praxis des »papiernen Königs« in der Kolonisation als auch den Registraturen der Kirchen im Mittelalter drücke sich der Wunsch aus, »die Welt in Schrift umzuwandeln«.

Mit der Französischen Revolution schließlich werde die Geburtenregistratur endgültig säkularisiert, erläutert Engemann.

»Gleichheit beginnt (...) mit dem unterschiedslos Registriertwerden. [...] Im weltlichen Regime der bürgerlichen Gesellschaft ist Bürger sein Geschriebenwerden.«

Die Namen seien dabei »Adressen für die Körper der Individuen«, die zentral sind für deren Regierbarkeit. Sei man ein Mensch ohne derartige Urkunde, Sans Papier, sei

man »nacktes Leben«, dem die »biopolitischen Zuwendungen (oder Zumutungen) [...] nicht zuteil werden«. Jeremy Benthams »An Introduction to the Principles of Morals and Legislation« sei Zeugnis einer fundamentalen Verschiebung vom Schreibakt in der Seele zum Schreibakt auf den Körper bis zum 18. Jahrhundert. Bentham nämlich weise auf die Namenstätowierungen der englischen Seeleute hin, um seine Forderung eines für jeden Menschen eindeutigen Namens zu untermauern. Dieser sollte nach seiner Vorstellung dem Individuum durch Registrierung ein Leben lang unauslöschlich zugeschrieben sein, wie eine Tätowierung. Tatsächlich werden in jener Zeit europaweite Verbote willkürlicher Namensänderungen, Zwänge zu eindeutigen Namen hinsichtlich des Geschlechts sowie Einschränkungen im jüdischen Namenssystem durchgesetzt.

»Geborenwerden ist unter Bedingungen neuzeitlicher Staatlichkeit keineswegs eine selbstverständliche Normalität, sondern ein Medienproblem.«

Engemann berichtet weiter von der Kampagne der Vereinten Nationen zur Verbreitung der Geburtenregistratur in Afrika und Asien: »Write me down, make me real«. Namentlich medial registriert zu sein in einer staatlichen Bürokratie werde hier eng verknüpft mit dem Existenzrecht an sich. Die Kampagne dient der Umsetzung der UN-Kinderrechtskonvention, in der in Artikel 7 die unverzügliche Eintragung jedes Kindes in ein Geburtenregister festgeschrieben ist. Die Kampagne soll beispielsweise Kinderhandel eindämmen oder Bürgerrechte

garantieren. Die Glücksversprechen, die mit einer Identitätsstiftung durch Registrierung verbunden werden, ähneln denen für die Einführung der an biometrische Daten geknüpften eindeutigen Registrierungsnummer Aadhaar durch die bereits oben erwähnte Unique Identification Authority of India (UIDAI). In ihren Werbefilmen propagiert sie nicht weniger als die Lösung des Armutsproblems: Aadhaar soll Zugänge zu staatlichen Leistungen oder zu einem Bankkonto unabhängig von der Kastenzugehörigkeit ermöglichen.

Ein weiterer nicht selten genannter Grund für derartige Registrierungskampagnen ist, dass sie der Namenlosigkeit der Opfer von und Täter in Gewaltverbrechen ein Ende bereite, die bei staatlichen Genoziden ein häufiges Problem im Zusammenhang mit der Straffreiheit der Täter darstellt.

Diese Argumente lassen sich allerdings auch ins genaue Gegenteil verkehren. Der massenhafte systematische Zugriff auf plötzlich unerwünschte Menschengruppen und deren Vernichtung setzt die Verunmöglichung jeglicher Anonymität voraus, wie der Holocaust grausam bewiesen hat.

Die Verwaltung von Namen und Körpern in Registern und damit des Lebens, ist gleichermaßen Bedingung für systematische Massengewaltverbrechen sowie für die Möglichkeit, jemanden dafür zur Verantwortung ziehen zu können. Ein fatales Dilemma der Moderne, das die Unmöglichkeit von Freiheit bedeutet.

Auch die digitale Welt bildet keine Ausnahme. Im Internet werde daher die eindeutige Adressierbarkeit über digitale Signaturen und Registraturen neu erzwungen.

»Was sich möglicherweise dabei verändert, ist das Verhältnis zwischen Körper, Grenze und Medien: Nicht mehr die Körper kommen zur Grenze und ihren Medien, die Medien kommen als Grenze zum Körper.«

Diese Prognose Engemanns ähnelt den Beobachtungen von Tsianos und Kuster in ihren Ethnografien der digitalen Grenze.

VIII. »Spoofing Biometrics in Science and Fiction – Geschichte(n) wider das unauslöschliche Siegel«¹⁵

So umfassend individuelle Identität, die staatlich kontrollierbar und verwaltbar ist, auch technisch hergestellt wird: »Das Unterwandern, Hintergehen und Austricksen biometrischer Systeme [ist] überhaupt kein neues Phänomen [...]«, schreibt Peter Bittner im Abstract zu seinem Vortrag. Im Gegenteil fänden sich zahlreiche Zeugnisse in Kriminalakten der Polizeien sowie in Filmen und Literatur bereits Anfang des 20. Jahrhunderts.

So seien in den FBI-Akten der 1930er und 1940er Jahre Versuche durch operative Veränderung der Muster, Verbrennung, Abrasion, Verätzung oder Transplantation dokumentiert. Besonders prominent seien die Fälle von John Dillinger oder Gus Winkler.

15 Vortrag von Peter Bittner am 30.11.12.

Mit einem anschaulichen Rückgriff auf eine große Sammlung inspirierender Quellen aus Filmen und Literatur, zurückreichend bis zur »Hightech-Methode zur Herstellung einer Gelatinefolie mit einem „falschen“ Fingerabdruck« im Roman »The Red Thumb Mark« aus dem Jahre 1907 von R. Austin Freeman, entwirft Bittner eine »Systematik der Überwindung«: von der Beseitigung und Vermeidung eigener Spuren, über »Elimination oder Veränderung des Merkmalsträgers zur Verschleierung eigener Spuren, die Wiederverwendung vorhandener Spuren« oder über deren Einbettung in einen anderen Kontext, die »Ent-Eignung« oder »Transplantation« fremder Merkmalsträger, bis hin zum Attrappenbau. Auch die Manipulation des biometrischen Systems selbst gehört letztlich dazu.

IX. »Identität ist Spurensuche«¹⁶

Der philosophische Blick Herbert Hrachovecs eröffnet einen Zugang auf wichtige Bedeutungsdimensionen des Begriffs Identität. Im Sinne der Hermeneutik beinhaltet er weniger die »Signifikantengleichheit«, »Identitätsfragen hängen [vielmehr] an Bedeutungsgleichheit«. Am Beispiel von Plagiaten macht der Autor dies schnell anschaulich: Auch ein paraphrasierter Wortlaut kann dasselbe bedeuten bzw. sogar dieselbe Aussage sein. Die »Messbarkeit« dieser Arten von gleicher Bedeutung er-

16 Vortrag von Herbert Hrachovec vom 1.12.12. Ausführlicher findet sich seine Argumentation im gleichnamigen Text dieses Bands, Seite 3.

fordere »Textverständnis«. Beim Wiedererkennen von Personen wiederum finde eine Identitätszuschreibung statt, die auf »Sinneseindrücken und Qualitätszuschreibungen beruht«.

Das in der Philosophie seit hunderten Jahren diskutierte Thema Identität werde bis heute recht unterschiedlich behandelt: Zwei Extreme sind zum einen die »formal-logische Rekonstruktion, [...] die No-Nonsense-Identität«, zum anderen »die Please-Let's-Have-Some-Nonsense-Interpretation, das ist die postmoderne Sichtweise«. Bei zweiterer Sichtweise ist laut Derrida »Identität Gleichheit in der Wiederholung«. Identität ist auf Zeitlichkeit verwiesen und »ist eher eine Defensivaktion [...] des Etwas-Aufgreifens und -Zugreifens in einem Ablauf, der in dieser Weise nicht gegeben ist.« Die Wiederholung desselben bedürfe »der Variation [und der] Annahme, in der Variation gibt es ein Sich-Durchhaltendes«.

Als logische Formen der Identität würden Reflexivität, Symmetrie und Transitivität gelten. Während tautologische, reflexive Aussagen selbstverständlich identisch seien, gehören symmetrische oder transitive Identitätsaussagen zu denen, »die nicht so sein müssen«. Auch biometrische Identität sei dieser Art. Es müsse gemessen werden. Es handelt sich dann um eine »empirische Identitätsaussage«. Ist es also wahr, dass $a=b$, dann ist b nichts anderes als a – die Person, auf die b sich bezieht, ist dann dieselbe, auf die a sich bezieht. Die Eigenschaftsbeschreibung eines Begriffes, die Intension, werde hier verwendet, um die Extension, den Umfang des Begriffs, zu bestimmen.

Der Begriff des Messens lasse sich aber sowohl aus dem No-Nonsense- als auch dem Nonsense-Approach darstellen: Es gibt Beobachter, einen beobachteten Prozess und ein Mess-System, das beides verbindet. Nach Bentley sei der Input einer Variable des Systems der »wahre Wert« derselben und der Output der gemessene Wert. Die Grundidee ist dabei, dass ein Mess-System verlässlich die Validität eines gemessenen Variablenwerts prüfen kann. Dazu wird ein Maßstab, eine Skala, benötigt.

»In Hegels Terminologie ergibt der Messvorgang, wie er gewöhnlich verstanden wird, Werte, die *für uns – an sich* sind. Anders gesagt: Wir stellen ein Ergebnis unserer Konstruktion als Ergebnis ohne unsere Konstruktion hin. [Hegel hat in] diesem dialektischen Moment etwas vorgesehen, was eine [...] Vorahnung der Dekonstruktion ist, also der Derrida'schen postmodernen Zugangsweise: nämlich die Empfehlung, etwas, was man als Position betroffen hat, immer auch zu hinterfragen. [...] Der Maßstab steht selbst auf dem Prüfstand.«

Das bringe zwar durchaus »die schöne Auswirkung« einer »Lernbereitschaft« mit sich, die aber auch korrumpieren könne. Dies geschieht, wenn »man den Maßstab dann doch nicht so ernst nimmt und ein bisschen nachkorrigiert aufgrund von Interessen, die man selber hat.«

Hrachovec versöhnt schließlich die formal-logische und die postmoderne Sichtweise auf Identität:

»Um feststellen zu können, ob zwei Gegebenheiten gleich sind, müssen Umstände gleich bleiben. Umstände sind auf andere Weise „gleich“ als Gegebenheiten.«

X. »Bildung zum emanzipatorischen Umgang mit Überwachungstechnologien«¹⁷

Den Messvorgang zu hinterfragen ist der so wichtige Zweifel, der ein Individuum weniger manipulierbar macht und dessen Fähigkeit, selbständig zu urteilen und klug zu entscheiden, befördert. Weder biometrische Systeme noch irgendeine andere Informationstechnologie sind unfehlbar. Dennoch werden Ausdrücke wie *das Internet*, *der Computer* oder *das IT-System*, die als abstrakte Sammelbegriffe für integrierte, komplexe Techniken stehen, zu Bezeichnungen sakraler Artefakte stilisiert. Sie gelten als Korrektiv des stets als problematisch angeführten menschlichen Versagens und flößen auf dieser Ebene gleichermaßen Furcht ein, denn menschliches Versagen ist aus eigener Erfahrung nachvollziehbarer als maschinelles. Versagen kann eine Sicherheitstechnologie per definitionem nicht. Jede Programmiererin einer Software für die Mustererkennung eines Biometriesystems aber weiß nur allzu gut, auf welch wackligen Füßen die Unfehlbarkeit ihres Programms steht. Die umfassenden Performanzmessungsstandards, komplizierten und selten öffentlich zu findenden konkreten Performanzstudien und halb-offiziellen Wettbewerbe um die besten Algorithmen einzelner Komponenten biometrischer Systeme sprechen Bände. Dennoch sind gerade die permanenten Ausbesserungen der Technologien Antrieb für ihr Wachstum, denn das Misstrauen in herkömmliche Praktiken der Personennidentifikation gepaart mit einem vermeintlich wachsen-

17 Vortrag von Andrea Knaut am 1.12.12.

den Sicherheitsbedarf ist fest in modernen, durch große Apparate verwalteten Organisationen wie Staaten, deren Behörden und großen Konzernen verankert.

Was müssen wir lernen über Biometrie, um ihr Umsichgreifen und dessen Auswirkungen zu begreifen und uns gegen die ihr inhärenten maschinellen Fehlentscheidungen schützen zu können? – Ausgangspunkt der Beantwortung dieser Frage ist, dass ein informatisches System niemals losgelöst von der menschlichen Gesellschaft beurteilt werden kann: Programmierbare Maschinen werden und wurden zur Lösung oder Bearbeitung menschlicher Probleme geschaffen, sie sind auch Projektionen von Wünschen und Hoffnungen. Dementsprechend erschließt sich ein großer Teil des Erfolgs der automatischen Personenerkennung historisch, wie es in einigen hier dokumentierten Vorträgen auch geschehen ist. Gegenwärtige und historische Analysen haben kulturelle, politische und soziale Dimensionen, geben Auskunft über die Machtverhältnisse zwischen zentralen Akteuren, die eine Technologie etablieren und stabilisieren. Im Falle der Biometrie spielen die Polizeien der modernen westlichen Nationalstaaten sowie Militär und Sicherheitsindustrie eine tragende Rolle.

Biometrische Systeme besitzen zahlreiche Angriffsvektoren – sich derer klar bewusst zu sein, verhindert das Ausgeliefertsein und das Ohnmachtsgefühl gegenüber einer solchen Technik. Es muss deutlich werden, dass die Macht der Technik nicht durch sie selbst, sondern durch einen gesamten institutionellen Apparat strukturell entsteht.

Ferner schafft die philosophische Annäherung ein besseres Verständnis für die Denk- bzw. Glaubensmuster, auf denen die moderne Vorstellung menschlicher Identität und ihrer Objektivierung durch Technologie beruht.

Bestandteile einer »Bildung zu einem emanzipatorischen Umgang mit Überwachungstechnologien«, wie es mit dem im Vortrag vorgestellten Schulprojekt getestet wurde, sind:

Erstens, die politische Durchdringung des Zusammenspiels von Sicherheit und Freiheit sowie der Kräfteverhältnisse einzelner Protagonistinnen verschiedener Sicherheitskonzepte, zweitens, die kulturellen Auswirkungen und, drittens, die Ursachen permanenter technologischer Überwachung und software-basierter Auswertung großer Datenmengen digitalisierter menschlicher Spuren. Viertens ist es von großer Bedeutung, die Technik selbst auszuprobieren, zu testen und zu manipulieren, um das praktische Begreifen ihrer Fehler zu ermöglichen. In einem solchen Bildungskonzept ist die komplette Infragestellung von Kontrolltechnologien möglich.

XI. »Verfahren der modernen, technisierten Personenidentifikation: massenhafte biometrische Erfassung«¹⁸

Das wirtschaftliche Wachstum der Firmen in der Biometrie-Branche seit 2001 stehe direkt mit der staatlichen Förderung in diesem Bereich durch das Bundesministerium des Innern (BMI), das Bundesministerium für Bildung

18 Vortrag von Constanze Kurz vom 1.12.12.

und Forschung (BMBF) oder das Bundesministerium für Wirtschaft und Technologie (BMWi) in Zusammenhang, insbesondere seit der sogenannten „Biometrie-Strategie“ der Bundesregierung seit 2005. Ein neueres Projekt im Rahmen dieser Strategie sei, berichtet Constanze Kurz, das Forschungsprojekt DigiDak, unter Beteiligung der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) der Uni Kassel, dessen Ziel »die Erforschung eines automatischen und rechtskonformen Systems zur Sicherung von Fingerabdrücken ist“.¹⁹

Das Wachstum des sicherheitstechnologischen Markts rund um die Biometrie liege über den von Frost & Sullivan in teuren Studien seit 2004 prognostizierten Zahlen – und dies trotz der Biometrie-Studien wie der BioP1- und BioP2-Studie des Bundesamts für Sicherheit in der Informationstechnik (BSI), des BMI und weiterer staatlicher und halbstaatlicher Einrichtungen, mit denen zentrale Argumente für die Verwendung der Fingerabdrücke in Passdokumenten widerlegt wurden. Die Technik habe dort alles andere als zuverlässig funktioniert.

Auch die »Ausweitung der Körpervermessung auf Kinder« für ein biometrisches Gesichtsbild im Kinderreisepass, die sowohl technisch unsinnig als auch ethisch hochbedenklich sei, sei derweil durchgesetzt. Bis heute unternehme die Industrie starke Lobbyarbeit in den Rechts- und Innenausschussanhörungen im Bundestag. Flughäfen seien nach wie vor die größten Abneh-

19 Vgl. Selbstbeschreibung „Bundesministerium für Bildung und Forschung: Digitale Fingerspuren (DigiDak) o. J.“ http://www.bmbf.de/pubRD/Mustererkennung_D_DigiDak.pdf, 24. 06. 2013.

mer für biometrische Kontrollsysteme. Ein zentrales Verkaufsargument sei hier die Beschleunigung der Grenzkontrolle, faktisch aber verlängerten sich die Zeiten durch ihren Einsatz: »Es sind [...] Sicherheitssimulationen, die hier aufgebaut wurden.«

Letztlich sei die Abgabe biometrischer Fingerabdrücke oder Gesichtsbilder für Pässe inzwischen alltäglich. Beim nPA würden inzwischen in ca. 30 Prozent der Fälle sogar freiwillig die Fingerabdrücke abgegeben.

Neuere Entwicklungen seien bspw. Körperscanner, die auch biometrische Technologien integrieren. Der 1000D-Whole-Body-Scanner von Iscon integriere Gesichts- und Iridenerkennung sowie kontaktbehaftete Fingerabdruckerkennung. Diese solle zukünftig aber auch kontaktlos geschehen.

Eine weitere wichtige Entwicklung in diesem Bereich sei die Explosion der DNA-Datenbanken von Straftätern, die im Rahmen des Prüm-Vertrags zwischen einzelnen EU-Staaten oder dem Abkommen zur Prävention und Bekämpfung schwerer Kriminalität zwischen den USA und einzelnen EU-Staaten neben anderen Daten ausgetauscht werden – Deutschland ist in beiden Fällen dabei. »DNA-Daten [...] werden natürlich wahrgenommen als perfekte biometrische Daten.«

In Großbritannien sei inzwischen ein Fünftel der Männer erfasst. Gerade bei DNA-Daten gibt es sehr

»wenig Gegenwehr und auch wenig Debatte – [die haben] dieses „Tatort“-Image: genetische Daten sind toll, da[mit] fängt man immer die Täter [...]. Für diese Datenbanken wie für alle gilt: Da gibt's eigentlich nur rein, aber nie raus.«

Auch der Consumer-Bereich wird von Kurz angesprochen: Dazu gehören viele verschiedene Anwendungen wie die viel diskutierten Schaufensterpuppen mit Gesichtserkennung, die Anmeldeschnittstellen an Laptops oder PCs via Gesichtserkennung oder Swipe-Sensoren, Wohnungsschlüssel oder Zündschlüssel. Sehr prominent diskutiert sei auch die Facebook-Gesichtserkennung. Diese sei durch die extrem breite Nutzung hochproblematisch. So würden »sechs Millionen Fotos pro Stunde« auch noch redundant abgelegt. Zwei Drittel der Fotos enthielten laut einer fragwürdigen amerikanischen Studie Gesichter.

Es würden sich jedoch immer wieder Praktiken der Gegenwehr anbieten. Sicherlich sei es sinnvoll, mit entsprechender Bildbearbeitung angepasste biometrische Bilder für die Ausweise abzugeben. Auch Fingerkuppen könnten Behandlungen erfahren, die deren Abgabe erschwert. Prinzipiell sei der europäische Reisepass im übrigen ohne funktionierenden Chip gültig. Bei Nachfragen müsse man standhalten. RFID-Chips könnten mit alten Mikrowellen zerstört werden (1000 Watt sind zu stark, besser 200 Watt, 20 Sekunden Maximum) oder mit sogenannten Zappern, die man selbst bauen könne, aber auch die mechanische Zerstörung durch gezieltes Heraufschlagen mit einem schweren Gegenstand sei vielversprechend.

XII. »EURODAC 2.0? Anmerkungen zur bevorstehenden Öffnung von EURODAC für Strafverfolgungsbehörden aus politikwissenschaftlicher Perspektive«²⁰

Die mit der neuen Eurodac-Verordnung²¹ ermöglichte Öffnung der Datenbank für den polizeilichen Zugriff stehe wie viele Überwachungstechnologien exemplarisch für den Function Creep einer einmal irgendwie derart etablierten Technologie. Jonathan Aus beantwortet die von ihm aufgeworfene Frage, warum der Zugriff interessant für Polizeien sei, entsprechend knapp:

»– weil Eurodac mittlerweile zwei Millionen biometrische Datensätze enthält [...], einfach, weil es zur Verfügung steht.«

20 Vortrag von Jonathan Aus vom 1.12.12.

21 Verordnung (EU) Nr. 603/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über die Einrichtung von Eurodac für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der Verordnung (EU) Nr. 604/2013 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist und über der Gefahrenabwehr und Strafverfolgung dienende Anträge der Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten und Europol's auf den Abgleich mit Eurodac-Daten sowie zur Änderung der Verordnung (EU) Nr. 1077/2011 zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts.

Die Frage, ob ein biometrisches Kontrollsystem wie Eurodac dabei wirklich die Lösung eines Problems (»rationalistische Sicht«) ist oder eine Lösung, die nach Problemen sucht (»institutionalistische Sicht«), werfe ein interessantes Licht auf die Art der »Institutionalisierung des ersten AFIS [Automatisiertes Fingerabdruckidentifizierungssystem] auf supranationaler Ebene«. In dieser spielen und spielten zahllose Akteure mit unterschiedlichem Einfluss und unterschiedlichen Interessen eine Rolle. Jonathan Aus hebt besonders das Bundesministerium des Innern oder kommerzielle Anbieter wie Sagem Défense Sécurité (heute Morpho) und das von Steria geführte Konsortium, das auch für das biometrische Visa-Informationssystem und die zweite Generation des Schengener Informationssystems zuständig sei, hervor.

Die zentrale Gesetzesgrundlage für die Etablierung von Eurodac ist, wie oben erwähnt, die sogenannte Dublin-II-Verordnung von 2003. Diese sei kaum im Interesse von EU-Grenzstaaten wie Griechenland oder Italien, die als sogenannte Verursacherstaaten mit Hilfe eines Instruments wie Eurodac viele Illegalisierte aus den Nordstaaten zurücknehmen müssten und dementsprechend wenige illegal Aufgegriffene überhaupt in der Datenbank registrierten. Die Dominanz bestimmter Nationalstaaten innerhalb der EU werde anhand der Asylpolitik sehr deutlich. Die »relative Macht« der einzelnen Staaten verteile sich innerhalb des Geflechts der verschiedenen EU-Institutionen wie u.a. Europäischer Rat, Europäische Kommission, Europäisches Parlament (rechtskonservative Mehrheit), Ministerrat, LIBE Committee, Ratspräsidentschaft,

der Asylum Working Party, den Botschaftern (Comité des représentants permanents) und dem Strategic Committee on Immigration, Frontiers and Asylum (SCIFA). Die langfristige Innen- und Sicherheitspolitik ergebe sich dann jeweils in auf einen bestimmten Zeitraum befristeten Programmen wie aktuell dem Stockholmer Programm, mit dem beispielsweise auch die Verfügbarkeit von Daten in nationalen AFIS oder DNA-Datenbanken sowie deren Austauschbarkeit sichergestellt wird. Es sind darin auch die Koordination von Abschiebeflügen oder militärische Flüchtlingsabwehr vorgesehen. Die systematische Harmonisierung der Migrationskontrolle wird innerhalb der EU verwaltungstechnisch als das Common European Asylum System (CEAS) bezeichnet. All dies biete sich in die sogenannten »internationalen Regime« wie Schengen, G6 oder den Vertrag von Prüm ein.

Bemerkenswert sei in diesem Kontext nicht zuletzt die sogenannte »agencyfication«, mit der die Gründung zahlreicher dezentraler EU-Agenturen per Verordnung bezeichnet wird. Die Agenturen dienen der Vernetzung nationaler Exekutivorgane, wie im Falle der Grenzpolizeien die European Agency for the Management of Operational Cooperation at the External Borders (Frontex). Ein anderes Beispiel ist die European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (IT Agency), die die Koordination der zahlreichen IT-Überwachungssysteme übernimmt. Inzwischen gibt es dreißig verschiedene solcher agencies. Ihre demokratische Legitimation ist umstritten.

Eurodac ist ein Teil dieses Netzwerks aus Staaten, Industrie, Lobbyorganisationen, Agenturen, Regimen, Abkommen, Verordnungen und IT-Systemen. Es ist ein unmenschliches System für die Betroffenen, die damit für die Nutzung eines eigentlich grundlegenden Menschenrechts auf Bewegungsfreiheit kriminalisiert werden.

»Ein zunehmendes Problem ist [... die] Selbstverstümmelung [...], „voluntary mutilation“ oder „wilful alteration“ von Fingerkuppen, verätzt oder verbrannt und insofern von Eurodac [...] nicht verwertbar. In Frankreich ist das offensichtlich gestiegen von 9% (2005) auf 14% (2011) [...] – [...] menschenrechtlich betrachtet eine durchaus problematische Tendenz, eine nicht intendierte Nebenfolge.«

Angesichts der erschreckenden Entwicklungen dieser unmenschlichen Politik der entpersonalisierten, automatischen Abweisung scheint eine gewisse Erinnerung vonnöten:

»Europas historische zivilisatorische Errungenschaft besteht sicherlich nicht darin, dass wir unsere Identität aus der Vermessung unserer Körper gewannen, sondern die Ideen von Menschenrechten und Demokratie zu institutionalisieren wussten.«

Redaktion: Andrea Knaut, Christian Ricardo Kühne

Satz: Andrea Knaut

Herausgeberin: Andrea Knaut,
Arbeitsgruppe Informatik in Bildung und Gesellschaft,
Institut für Informatik, Humboldt-Universität zu Berlin.
Mit freundlicher Unterstützung durch die
Alcatel-Lucent-Stiftung.



Alcatel-Lucent
Stiftung für
Kommunikations-
forschung



INFORMATIK IN
BILDUNG &
GESELLSCHAFT



erschienen: August 2013

Lizenz der Texte: Texte unterliegen Creative Commons bei Namens-
nennung der Autor_innen und nicht-kommerzieller
Nutzung



The texts are licensed under a Creative Commons
Attribution NonCommercial 3.0 Germany License.